# Department of Homeland Security Daily Open Source Infrastructure Report for 22 May 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

**Daily Highlights**

- KDKA reports investigators are trying to determine how a small explosive device got past security at Pittsburgh International Airport and was then set off inside a magazine store. (See item 14)
- The New York Times reports as many as 85,000 large residential and commercial buildings in New York City lack special valves on their water connections that could prevent hazardous substances from being pulled into the public water system. (See item 21)
- The Associated Press reports a gunman suspected of killing three people and himself in Moscow, Idaho, on Sunday, May 20, had said during a court−ordered mental evaluation that if he committed suicide, he would try to take a large number of people with him. (See item 28)

**DHS Daily Open Source Infrastructure Report *Fast Jump***



## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *May 21, Electric Light & Power* — **Con Edison launches Project Hydra to enable secure super grids.** Consolidated Edison Inc. has contracted American Superconductor Corp. to develop and deploy a new high temperature superconductor (HTS) power grid technology in Con Edison's New York City power delivery network. The Department of Homeland Security

(DHS) is expected to invest up to $25 million in the development of this technology to enable "secure super grids" in the U.S. Secure super grids utilize customized HTS wires, HTS power cables and ancillary controls to deliver more power through the grid while also being able to suppress power surges that can disrupt service. Jay M. Cohen, DHS under secretary for science and technology, said "As we saw with the August 2003 blackout and in incidents since, disruptions to the power grid have far−reaching effects and a tremendous economic impact. We have asked AMSC and Consolidated Edison to demonstrate superconductor solutions in New York City that will serve to keep our centers of commerce on line under all conditions −− including grid events related to severe weather, accidents or terrorist attacks." Code named "Project Hydra" by DHS, multiple paths for electricity flow will be created in power grids to ensure system reliability if circuits were to be disrupted.
Animation of Secure Super Grids: http://www.amsc.com/products/hydra.cfm
Source: http://uaelp.pennnet.com/display_article/293206/22/ARTCL/none/none/Con−Edison−launches−

2. *May 19, Toledo Blade (OH)* — **Regulators skeptical of Davis−Besse report.** A 661−page report that FirstEnergy submitted to its insurance company in hopes of recouping $200 million for the near−rupture of Davis−Besse's old reactor head in 2002 is being viewed by the Nuclear Regulatory Commission's enforcement office "with skepticism," according to a document filed in federal court late Friday, May 18, by the U.S. Department of Justice. The Justice Department acknowledged for the first time that contradictions between the position of FirstEnergy's new consultants and previous government research "appear to be particularly significant." "It appears that the [new] Wastage Event report [written by FirstEnergy's consultants] arrives at its conclusions by selectively ignoring contrary evidence," U.S. Attorney Greg White and three other federal prosecutors said in their joint filing in a case being heard by U.S. District Judge David Katz of Toledo. The case involves two former Davis−Besse engineers and an outside contractor accused of lying to the government about the plant's dangerous condition in the fall of 2001. Each defendant faces up to five years in prison and $250,000 in fines if convicted.
Source: http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20070519/NEWS06/705190401

3. *May 18, Houston Chronicle* — **Delivering is called key for alternative fuels.** Alternative energy isn't the next big thing. That's because it's already here, an analyst told energy executives at a conference in Houston on Friday, May 18. The key for the ever−growing alternatives sector is to deliver, particularly when the current political environment is encouraging and high energy prices make such investments more economical, Simmons & Company International analyst Pearce Hammond said. "I firmly believe the biggest challenge alternative energy has in front of it now is to execute," he said. Pamela Beall of Marathon Oil Corp. said technology to create more ethanol from non−food sources is years away. The nation's pipelines and other energy infrastructure cannot transport biodiesel, so it must be moved by truck or rail. Alan Forster of Shell WindEnergy said a hindrance to growth includes a stressed infrastructure. While 1.5 percent of the total energy generation worldwide comes from wind, the U.S. is a growth market, and wind pro− jects are economically viable with subsidies, Forster said. The same is said of biofuels. But he said investment in energy transmission is needed to keep up with growth and demand. "We have not invested in transmission in the United States in 20 years," he said.
Source: http://www.chron.com/disp/story.mpl/business/4817954.html

[Return to top]

## Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

## Defense Industrial Base Sector

4. *May 21, Government Accountability Office* — **GAO−07−803R: Defense Infrastructure: Full Costs and Security Implications of Cheyenne Mountain Realignment Have Not Been Determined (Correspondence).** The Department of Defense (DoD) built the Cheyenne Mountain Operations Center located near Colorado Springs, CO, in the early 1960s to withstand a multimegaton−yield−weapon strike and to provide protection against chemical and biological warfare. The mission of the Cheyenne Mountain Directorate is to monitor, process, and interpret air, missile, and space events that could threaten North America or have operational effects on U.S. forces or capabilities. This mission is conducted at five major centers −− the Command Center, Air Warning, Missile Correlation, Operations Intelligence Watch, and Space Control −− all currently located within Cheyenne Mountain. Elements of United States Strategic Command and Air Force Space Command are also located in Cheyenne Mountain. The Government Accountability Office (GAO) was asked to determine (1) the estimated costs, savings, and benefits associated with moving functions from Cheyenne Mountain to other locations; and (2) how DoD evaluated the security implications associated with moving the functions, and what these implications are. On March 13, 2007, GAO delivered a briefing on preliminary observations regarding the proposed relocation. This report summarizes the results of that briefing and provides updated information as a result of additional work GAO has performed since that time.
Source: http://www.gao.gov/new.items/d07803r.pdf

[Return to top]

## Banking and Finance Sector

5. *May 21, Computerworld Australia* — **XML format for antiphishing info to go live in July.** A common format to electronically report fraudulent activities will be fully operational by July 2007. Anti−Phishing Working Group (APWG) secretary general, Peter Cassidy, said a structured data model is necessary to improve incident reporting, share information and allow forensic searches and investigations. Cassidy said the first base specification was submitted in June 2005 and the Incident Object Description Exchange Format (IODEF) XML Schema with e−crime relevant extensions will be a recognized IETF standard in about six weeks. He said reporting will be automated with greater ease using a standard schema. "For example, a Korean CERT (Computer Emergency Response Team) reporting an incident can send it to a French bank," he said. Cassidy said the APWG first started collecting data in October 2003. To date, he said 2.5 million records of attacks and 13,500 URLs are added to the database every month. Cassidy said the block list is updated every five minutes and is a 10MB file used as a historical

archive, most commonly used by browser developers. URLs are sent by banks, institutions, retailers, CERTs and volunteer organizations.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9020062&intsrc=hm_list

6. *May 20, Oregonian* — **Prosecutors say woman laundered $4 million with untaxed cigarettes.** Federal prosecutors want to seize nearly $4 million from a Washington state woman indicted on cigarette trafficking and money laundering charges. A U.S. District Court grand jury handed up a 62−count indictment last week accusing Joann Cook of laundering nearly $4 million from sales of untaxed cigarettes through her J&J's Smokeshop in Okanogan from 1999 to 2006. James A. McDevitt, U.S. attorney for Eastern Washington, has estimated that Washington state lost about $56 million in tax revenue in schemes to bring untaxed cigarettes from Indian reservations in Idaho. The indictment seeks forfeiture of more than $3.9 million: the amount federal prosecutors allege Cook laundered from September 1999 to May 4, 2006, when federal and state agents raided the business. Reservation smoke shops can legally sell untaxed cigarettes only to tribal members. In Washington, the state tax amounts to $14.25 a carton. The indictment also seeks the forfeiture of contraband cigarettes, more than $8,300 from a bank account, more than $20,000 in seized cash, as well as a $3.9 million judgment representing the laundered money. Several federal and state law enforcement agencies joined to investigate the untaxed cigarette scheme.
Source: http://www.oregonlive.com/news/oregonian/index.ssf?/base/news/1179550526299220.xml&coll=7

7. *May 20, Associated Press* — **Company hired to check lottery security not checked.** A company hired to audit the security systems of the North Carolina Lottery wasn't checked by state officials, who would have found that the company isn't registered to do business in the state, The Charlotte Observer reported Saturday, May 19. Tidwell Dewitt LLC of Alabama was picked to check computer systems that allow printing of lottery tickets at stores and other locations. The company has also been named in a $4 million negligence lawsuit in Atlanta, claiming that it failed to find an embezzlement at a company whose books it audited for years. Tidwell official Drew Sipos said that Tidwell didn't have to register because a computer−services company is handling the audit for it, not an accounting company. Sipos also said that the lawsuit filed in Atlanta was meritless. But Robert Brooks, the executive director of the state Board of CPA Examiners, said that any company hired to work in North Carolina has to register.
Source: http://www.journalnow.com/servlet/Satellite?pagename=WSJ%2FMGArticle%2FWSJ_BasicArticle&c=MGArticle&cid=1173351272752&path=!localnews&s=1037645509099

8. *May 20, Reuters* — **CIA briefing SEC monthly on terrorists: Barron's.** The U.S. Securities and Exchange Commission (SEC) is being briefed monthly by the Central Intelligence Agency (CIA) about terrorists and other criminals active in global stock markets, Barron's said in its latest edition. Barron's said SEC Chairman Christopher Cox told the publication he and four other commissioners are briefed each month and that the CIA reports offer the SEC a "somewhat sharper focus" to an "underworld of murky, illegal dealings that threaten the world capital markets." They are the first regular intelligence briefings for the SEC in history, Barron's said in its May 21 edition. "The U.S. government's focus on money laundering and

terrorist financing and other criminal activities in the capital markets has laid bare a good deal of activity of that sort," said Cox, who would not confirm whether terrorists were active or present in U.S. markets.
Source: http://news.yahoo.com/s/nm/20070520/bs_nm/sec_cia_briefings_dc;_ylt=Apb15nWjxLiXhfmDQ57990YjtBAF

9. *May 19, Stony Brook Independent (NY)* — **Personal information of up to 90,000 compromised at Stony Brook University.** The personal information of 90,000 people in a Stony Brook University database was accidentally posted to Google and left there until it was discovered almost two weeks later. According to a Website set up by the university, Social Security numbers and university ID numbers of faculty, staff, students, alumni, and other members of the community were visible on Google after they were posted to a Health Sciences Library Web server on April 11. The files were not easily accessible through Google and the "information could only be retrieved through the use of multiple criteria." The New York State Cyber Security Office contacted Google to have the information removed after it was discovered on April 24.
Source: http://www.sbindependent.org/node/1850

10. *May 19, Computerworld* — **New and improved version of Gozi Trojan horse on the loose.** A new, stealthier version of a previously known Russian Trojan horse program called Gozi has been circulating on the Internet since April 17 and has already stolen personal data from more than 2,000 home users worldwide. The compromised information includes bank and credit card account numbers (including card verification value codes), Social Security numbers and online payment account numbers as well as usernames and passwords. As with its predecessor, the new version of Gozi is programmed to steal information from encrypted Secure Sockets Layer (SSL) streams and send the stolen information to a server in Russia. The new version is very similar to the original Gozi code in its purpose, but features two core enhancements. One of them is its use of a new and hitherto unseen "packer" utility that encrypts, mangles, compresses and even deletes portions of the Trojan horse code to evade detection by standard, signature−based antivirus tools. The original Gozi, in contrast, used a fairly commonly known packing utility called Upack, which made it slightly easier to detect than the latest version. This version of Gozi also has a new keystroke−logging capability for stealing data, in addition to its ability to steal data from SSL streams.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019978&intsrc=hm_list

11. *May 18, Sophos* — **Fake digital camera order spam hits Australia.** A widescale spam campaign hit e−mail inboxes this week. The emails, which claim to come from Dell's online store, appear to have been deliberately targeted at Australian Internet users and say that an order for an AU $805 Canon digital camera has been accepted and the recipient's credit card will be duly charged. Visiting the link contained inside the e−mail, which is presented as a numerial IP address rather than a more usual name, could potentially infect the user's computer with a malicious code or take them to a Website designed to steal information for the purposes of identity theft. Dell Australia has published a warning about the email on its Website, confirming that they have not sent the e−mails and that users should be on their guard. Sophos has been proactively blocking access to the Website referred to in the email since 24 April 2007 with its Web security appliance.

Source: http://www.sophos.com/pressoffice/news/articles/2007/05/dell .html

[Return to top]

## Transportation and Border Security Sector

**12.** *May 21, Associated Press* — **Low−cost Skybus prepares for inaugural flight.** The success or failure of a new discount airline depends on whether some travelers are willing to fly to smaller, secondary airports and then drive 30 minutes or more to reach destinations such as Boston or Seattle, analysts say. Skybus Airlines is scheduled to make its inaugural flight Tuesday, May 22, entering the often stormy industry of low−cost air travel. The company has plans to fly to 25 cities from its hub at Ohio's Port Columbus International Airport, using a model aimed at competing with Southwest and other no−frills airlines. Every Skybus flight will offer at least 10 tickets for $10 each. More than 200,000 tickets have already been sold −− tickets are booked solely through the company's Website to save costs, part of a business strategy that also includes charging passengers for added services. Priority boarding will cost $10, and sandwiches and salads will cost up to $10. Skybus officials said they see an opportunity to draw would−be passengers from Cleveland, Cincinnati and as far as Fort Wayne, IN, and Charleston, WV.
Source: http://www.usatoday.com/travel/flights/2007−05−21−skybus−lau nch_N.htm

**13.** *May 21, USA TODAY* — **Airport check−in: Higher fees challenged in Los Angeles.** A judge for the Department of Transportation determined last week that the higher fees Los Angeles International Airport (LAX) imposed on the airlines are "unreasonable," a setback for the city's airport officials who are looking to raise money for major renovation. Last December, Los Angeles World Airports, the city agency that operates LAX, sharply raised rent and maintenance fees for the 28 airlines at Terminals 1 and 3 and Tom Bradley International Terminal, most of them low−cost or international carriers. The airlines appealed to the DOT, arguing the increase would result in higher fees passed onto customers and, ultimately, a cutback in service. U.S. Administrative Law Judge Richard Goodwin found the increased charges "discriminate" against the complaining airlines. He called for refunds to the airlines for fees already paid. His ruling is not binding but will be considered by the Department of Transportation, which issues its final ruling June 15. "We are gratified by today's recommended decision," said some of the carriers, including Southwest, Alaska, US Airways, Frontier and AirTran, in a joint statement. Airport officials contend the increase is necessary because the airlines pay only a fraction of the costs needed to run the terminals and maintain security.
Source: http://www.usatoday.com/travel/flights/2007−05−20−airport−ch eckin_N.htm

**14.** *May 21, KDKA (PA)* — **Explosive device found at Pittsburgh International.** Investigators are trying to determine how a small explosive −− possibly homemade −− device made it past security inside Pittsburgh International Airport. The device was set off inside an airside magazine store. Sources say the device, which was about the size of a shotgun shell, was wrapped tightly in paper. When it went off, it sounded like a firecracker. No one was hurt. Allegheny County's Explosion and Demolition team is right now taking a look at the device to determine what it is made of. Meantime, an airport operations employee has been fired after another security breach at the airport. Last month, airport security saw a man scale a fence and drop into the cargo area.

Source: http://kdka.com/topstories/local_story_137164938.html

15. *May 20, USA TODAY* — **Mass−transit building boom begins in Manhattan.** The quest for a subway to carry commuters along Manhattan's Second Avenue was first proposed in 1920 but was beset by financial problems over the years. Now, much of the funding is in place for at least the initial phase of construction, and ground was broken last month for the elusive subway line. In New York City, transportation projects that are planned or underway include extension of subway service to the far West Side of Manhattan, possibly hastening commercial and residential development in the area. Also on tap: a new Long Island Railroad terminal at Grand Central Station in Midtown and a transit center in Lower Manhattan that will make a labyrinth of subway entrances easier to navigate. Concerns about high gasoline prices, congested roads and the growing number of aging drivers who eventually may need other ways to get around are compelling voters across the country to approve ballot measures that create transportation plans and raise taxes to pay for such projects. Some cities are building transportation networks for the first time, while others are ramping up systems that have been in place for decades.
Source: http://www.usatoday.com/news/nation/2007−05−20−mass−transit− boom_N.htm

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

16. *May 20, Associated Press* — **Disease−spreading bugs could wipe out Arizona's oleanders.** A centimeter−long insect is threatening to destroy an iconic Arizona plant. The smoke−tree sharpshooter is spreading a disease−causing bacterium that is killing oleanders in north−central Phoenix. And scientists don't know when or if it will stop. Sharpshooters and oleanders have lived in harmony in Arizona for decades, but the bacterium is the problem. Authorities believe it came to Arizona on a vegetation truck from California. The disease caused by the bacterium is known as oleander leaf scorch. It gets into the plant's vascular system and prevents water from reaching the outer branches.
Source: http://www.kold.com/Global/story.asp?S=6541966

17. *May 19, Associated Press* — **Diseased cows worry Montana.** Seven cows traced to a ranch in the southern part of the state have tested positive for the livestock disease brucellosis, state officials said Friday, May 18. If a second herd is found to have the disease, which causes pregnant cattle to abort their calves, Montana could lose its brucellosis−free certification from the federal government. That would force a prolonged and costly testing and vaccination program for the state's 2.5 million cattle, state officials and industry representatives said. The source of the Bridger outbreak is under investigation by state and federal agriculture agents. State officials said that will include testing of other herds that might have come into contact with the diseased one to determine if the brucellosis has spread. Idaho lost its brucellosis−free status in 2005 and has yet to regain it. The only other state not brucellosis−free is Texas.

Source: http://www.rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_5544857,00.html

18. *May 19, Advocate (LA)* — **Crawfish disease source sought.** Louisiana officials have begun widespread testing to identify the source of a crawfish virus that was identified in two more ponds the week of May 18. White spot disease, which could threaten the state's crawfish crop, was first confirmed last week in two ponds at a crawfish farm near Arnaudville on the line between St. Martin and St. Landry parishes. Commissioner of Agriculture and Forestry Bob Odom said Friday, May 18, that further testing has found the disease in two more ponds in Vermilion Parish. The four ponds are under quarantine, and the agriculture department has begun testing crawfish delivered to all peeling plants in the state, Odom said. Peeling plants receive crawfish from several ponds, so sampling incoming crawfish will give officials a good idea of how widespread the disease is, Odom said. The state Department of Wildlife and Fisheries has begun testing wild crawfish from the Atchafalaya Basin. Wildlife and Fisheries Inland Fisheries Program Manager Charlie Dugas said crawfish samples were collected Tuesday from crawfishermen at boat landings on both sides of the Basin, the source of most of the wild crawfish caught in the state.
Source: http://www.2theadvocate.com/news/7586437.html

19. *May 18, Science* — **Case of the empty hives.** David Hackenberg was the first beekeeper to draw attention to what is now one of the hottest problems in agriculture: a devastating collapse of honeybee colonies. Last October, while inspecting 400 of his company's hives in Florida, he noticed that 368 were almost empty, despite having been healthy just three weeks earlier. Gone were the swarming worker bees; instead, the eerily quiet hives housed just the queen bee and many doomed brood. All told, Hackenberg has lost 85 percent of his 3000 hives. Alarmed, Hackenberg contacted Diana Cox−Foster, an entomologist at Pennsylvania State University (PSU). Soon she and Dennis vanEngelsdorp, the state apiarist, heard of similar problems from beekeepers across the country. By January, the two had established a network of researchers from Florida to Montana to solve the puzzle of what they're calling colony collapse disorder (CCD). "It's a science−fiction scenario come to life," says entomologist May Berenbaum of the University of Illinois. Some scientists now fear that the emergence of CCD will tip the balance, forcing many beekeepers out of business and raising costs for farmers who already rent hives because of a lack of natural pollinators.
Source: http://www.sciencemag.org/cgi/content/full/316/5827/970

[Return to top]

## Food Sector

20. *May 20, Chicago Tribune* — **Big holes frustrate food import safety net.** No country highlights the gaps in America's food import system as much as China, a rapidly industrializing, mass−exporting country whose food safety controls lag those of Western nations. In April alone, the U.S. Food and Drug Administration (FDA) turned back 257 Chinese import shipments, far more than from any other country, FDA records show. At least 137 of them involved food rejected for reasons like "filthy," "salmonella," or because it contained banned ingredients. A good portion of the rejected Chinese shipments each month includes fish and seafood, such as catfish, shrimp, mahi−mahi, tilapia, eel and yellowfin tuna. Other Chinese

imports that did not get past inspectors included herbal teas, bean curd, candy, dried apples, dried peaches and peanut milk. The FDA is rushing to adapt. Earlier this month the agency established a new post, assistant commissioner for food protection. David Acheson has launched a review of food safety practices. "The agency is heavily focused on what you might call reactive mode," Acheson said. "Where and when we see a problem, we react to it. The inspections that we do are risk−based, target areas that we think are higher risk. The big area we need to do more on is the prevention phase."
Source: http://www.chicagotribune.com/news/nationworld/chi−food_bdmay20,1,1045418.story?coll=chi−newsnationworld−hed

[Return to top]

## Water Sector

**21.** *May 19, New York Times* — **Thousands of buildings lack required water valve, New York records show.** As many as 85,000 large residential and commercial buildings in New York City lack special valves on their water connections that could prevent hazardous substances from being sucked into the public water system, according to city records. In investigating the presence of a chemical, tetrachloroethylene, in the drinking water supply in parts of Queens, city officials identified a car wash as having contributed to the contamination at least partly because it did not have the valve installed on one of its water supply lines. The amount of the contaminant was considered too low to pose a serious health problem. The records also show that about 26,000 buildings in the city represent an especially high risk because factories, gasoline stations or businesses that handle hazardous materials have not installed the device, called a backflow prevention valve. State law has required that the device be installed on certain categories of buildings since 1981. The backflow prevention valves are generally located near water meters inside commercial, industrial and large residential buildings. They are attached to water lines completely separate from wastewater lines that run to the sewers, and are designed to prevent contaminated water within a building's systems from being drawn back into the water mains.
Source: http://www.nytimes.com/2007/05/19/nyregion/19water.html?_r=1 &oref=slogin

[Return to top]

## Public Health Sector

**22.** *May 21, Xinhua (China)* — **Second child dies in hand−foot−mouth outbreak in east China city.** A 14−month−old child has died of hand−foot−mouth disease in Linyi city, in east China's Shandong Province, bringing the death toll in the outbreak to two, the provincial health department has announced. The baby boy was admitted to Linyi People's Hospital on Saturday, May 19, after developing symptoms of fever and a rash with blisters, said a spokesperson of the department. A two−year−old girl −− also diagnosed with hand−foot−mouth disease −− died in hospital on April 29. The city has reported 981 cases of hand−foot−mouth disease since April, 609 of whom have recovered, according to the department. Shandong recorded 2,477 cases of hand−food−mouth disease in 2005, including one death, and 3,030 cases in 2006, two of which were fatal.

Hand−foot−mouth disease information:
http://www.cdc.gov/ncidod/dvrd/revb/enterovirus/hfhf.htm
Source: http://english.people.com.cn/200705/21/eng20070521_376540.ht ml

**23.** *May 21, Xinhua (China)* — **Bird flu outbreak leads to mass cull.** China's Ministry of Agriculture confirmed on Saturday, May 19, that an outbreak of H5N1 bird flu at Shijiping Village in Yiyang city of Hunan Province has killed more than 11,000 head of poultry. The Ministry of Agriculture and the Hunan provincial government implemented an emergency plan to deal with the outbreak, culling a further 52,800 birds to prevent any spread of the disease. Agriculture officials say that the outbreak has been brought under control. The last reported cases occurred on March 1, when a batch of chickens suddenly died in a market in Lhasa, capital of Tibet Autonomous Region.
Source: http://www.shanghaidaily.com/sp/article/2007/200705/20070521 /article_316547.htm

**24.** *May 20, Reuters* — **Bangladesh launches emergency polio vaccination drive.** Bangladesh began immunizing two million children against polio on Sunday, May 20, in an emergency vaccination drive in a southeastern region close to Myanmar, officials said. The campaign follows confirmation that a polio−infected child from Myanmar had travelled to Chittagong and Cox's Bazar for treatment in March. "The children will receive a first round of vaccinations on Sunday and the concluding second round will take place on July 1," a government health department official said. The vaccination drive is taking place in Chittagong, Cox's Bazar and Bandarban districts bordering Myanmar's Rakhine (Arakan) state.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.alertnet.org/thenews/newsdesk/DHA100463.htm

**25.** *May 20, Sky News (United Kingdom)* — **Police investigate oxygen tampering.** Police have launched an investigation after it was revealed oxygen cylinders at a hospital may have been maliciously tampered with. The alarm was raised after staff transporting a patient within Sandwell General Hospital in West Bromwich, United Kingdom, noticed a solid substance was blocking the flow of oxygen to his face mask. Managers ordered the hospital's entire stock of several hundred portable cylinders to be checked for defects. It was then discovered two other cylinders, which were available for patient use, had also been blocked by an unidentified substance. All three cylinders had been apparently tampered with on the outlet from the regulator.
Source: http://news.sky.com/skynews/article/0,,30100−13586711,00.htm l

[Return to top]

## Government Sector

**26.** *May 21, YourHub.com (CO)* — **Colorado school district looking at new camera technology.** The Douglas County School District is looking into purchasing new technology that allows law enforcement to look inside schools through cameras in the event of an emergency situation. The system allows officers to plug into the school's cameras and view images within minutes of arrival on an emergency, allowing them to get a real−time view inside the school. In some cases, officers would be allowed to zoom in and out and pan from side to side with some of the

cameras. The video footage is picked up through a powerful antenna placed on the roof of the school. The images are then relayed to a command center or a computer in the officer's patrol car. Although the cameras can't cover every square inch of the school, it would give officers a significant advantage in the event of an emergency, said Larry Borland, executive director of safety and transportation.
Source: http://denver.yourhub.com/CastleRock/Stories/News/Law/Story~ 311308.aspx

**27.** *May 21, Department of Homeland Security* — **DHS completes key framework for critical infrastructure protection.** The Department of Homeland Security announced on Monday, May 21, the completion of 17 Sector−Specific Plans (SSPs) in support of the National Infrastructure Protection Plan (NIPP). The NIPP outlines a comprehensive risk management framework that defines critical infrastructure protection roles and responsibilities for all levels of government and private industry. Homeland Security Presidential Directive 7 identified 17 critical infrastructure and key resource sectors that require protective actions to prepare for, or mitigate against, a terrorist attack or other hazards. The sectors are: agriculture and food; banking and finance; chemical; commercial facilities; commercial nuclear reactors, including materials and waste; dams; defense industrial base; drinking water and water treatment systems; emergency services; energy; government facilities; information technology; national monuments and icons; postal and shipping; public health and healthcare; telecommunications; and transportation systems including mass transit, aviation, maritime, ground or surface, rail and pipeline systems. The vast majority of the nation's critical infrastructure is owned and operated by private industry. SSPs define roles and responsibilities, catalog existing security authorities, institutionalize already existing security partnerships, and establish the strategic objectives required to achieve a level of risk reduction appropriate to each individual sector. National Infrastructure Protection Program Sector−Specific Plans Fact Sheet: http://www.dhs.gov/xnews/gc_1179776352521.shtm
Source: http://www.dhs.gov/xnews/releases/pr_1179773665704.shtm

**28.** *May 21, Associated Press* — **Idaho shooter spoke of killing others.** A gunman suspected of killing three people and himself said during a court−ordered mental evaluation that if he committed suicide, he would try to take a large number of people with him, police said Monday, May 21. Three months after that conversation with a psychiatrist, authorities say, Jason Hamilton shot and killed his wife at her home, then toted two assault rifles to a parking lot and fired a barrage of bullets into an emergency dispatch center across from a Moscow, ID, courthouse. A police officer rushing to the scene late Saturday was killed, and a deputy and a civilian who tried to help were wounded. Investigators said Hamilton, 36, also killed sexton Paul Bauer, 62, in an office of the nearby the nearby First Presbyterian Church early Sunday, May 20. Officers who stormed the church hours later found a rifle and ammunition next to Hamilton's body in the sanctuary. Hamilton had a history of violence, and a judge ordered him evaluated after he tried to kill himself, Assistant Police Chief David Duke said. Moscow, home of the University of Idaho, is located 80 miles south of Spokane, WA, and surrounded by vast farmland.
Source: http://hosted.ap.org/dynamic/stories/I/IDAHO_SHOOTINGS?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

[Return to top]

# Emergency Services Sector

**29.** *May 20, Fox 13 News (FL)* — **First responders in Florida practice for disaster.** Hurricanes, terrorist attacks, and even wildfires: whatever the disaster, emergency crews will tell you it takes training and preparation to save lives. With hurricane season just two weeks away, first responders in Manatee County, FL, are getting ready. They trained at the Port of Manatee in an area that they call 'Ground Zero.' They removed wrecked cars, downed trees, and power lines that littered roads as part of the series of exercises. Twenty different agencies from all over Manatee County came together to work as a team.
Source: http://www.myfoxtampabay.com/myfox/pages/News/Detail?contentId=3258967&version=2&locale=EN−US&layoutCode=TSTY&pageId=3.2 .1

**30.** *May 20, WTKR−TV (VA)* — **Interstate lane reversal drill in Virginia.** Hurricane season kicks off June 1, and Hampton Roads, VA, emergency workers want to make sure residents can get out of the area safely in the event a major storm. For the first time, officials tested the ability to reverse the lanes on I−64. The eastbound lanes from Richmond to Newport News were reversed around 5:00 p.m. EST Sunday morning, May 20. Virginia Department of Emergency Management says sooner or later Hampton Roads will face an event that calls for mass evacuations and they know that communication is key with other agencies like Virginia State Police, Virginia Department of Transportation, and the Virginia National Guard. For the first time, agencies closed down on−ramps to I−64 as a part of a drill. They lowered the hurricane gates to test interstate reversal. If it were a real evacuation, whether it be a major storm, terrorist attack, or other disaster, agencies would quickly close 36 on−ramps between Hampton Roads and Richmond and make every lane westbound on both sides of the interstate −− moving all traffic away from Hampton Roads.
Source: http://www.wtkr.com/Global/story.asp?S=6541484&nav=ZolHbyvj

**31.** *May 20, Associated Press* — **Three guilty of FEMA fraud.** Three people have been sentenced in federal court in Biloxi, MS, on charges of illegally receiving disaster payments from the Federal Emergency Management Agency (FEMA) for debris cleanup after Hurricane Katrina. Clinton K. Miller of Carrier and Lauren Robertson of Picayune, who both worked for a debris monitoring company, were sentenced to 33 months and 13 months, respectively. Each was ordered to pay $275,057 in restitution. Allan Kitto of Dundee, FL, owner and operator of J.A.K. DC&ER Inc., worked under a subcontract as a debris hauler. He was sentenced to 25 months in jail and a $275,057 fine. The three pleaded guilty in February to conspiracy involving submission of $716,677 in false debris hauling tickets.
Source: http://www.hattiesburgamerican.com/apps/pbcs.dll/article?AID=/20070520/NEWS01/705200341/1002

[Return to top]

# Information Technology and Telecommunications Sector

**32.** *May 21, IDG News Service* — **Mobile provider Alltel agrees to $27.5B buyout.** Mobile phone and wireless services provider Alltel on Sunday, May 20, agreed to a $27.5 billion buyout, a deal likely to spur more such acquisitions in North America. The company, which

serves 12 million mobile phone subscribers in 35 states, signed a deal to be bought by TPG Capital, and the private equity division of Goldman Sachs Group.
Source: http://www.infoworld.com/article/07/05/21/Alltel−agrees−to−b uyout_1.html

**33.** *May 21, CNET News* — **Expert: IT industry has failed in desktop security.** The IT industry has failed when it comes to desktop security for all major operating systems, a security specialist told delegates attending a security conference in Australia. Ivan Krstic, director of security architecture for the One Laptop per Child project, kicked off the AusCert 2007 conference Monday morning, May 21, with a keynote speech that blasted desktop computer security because it is based on a 35−year−old premise where software can run with the same privilege as a user. "The number one broken assumption of desktop security...is this very simple premise that all executing software should execute with the full permission that its user possesses," Kristic said. "There are a bunch of programs that ship with all major operating systems −− including Linux, Mac OS and Windows −− that can format your hard drive, spy on your computer, spy on you with your microphone and camera, and turn over control of your computer to third parties," said Krstic.
Source: http://news.com.com/Expert+IT+industry+has+failed+in+desktop +security/2100−1002_3−6185295.html

**34.** *May 21, VNUNet* — **Bad Norton update zaps 'millions' of PCs.** A faulty update to Symantec's Norton Antivirus package has disabled "millions" of PCs in China, according to local press reports. One report carried by China's official news agency put the number of affected PCs in the millions, although others said that the figure was more like thousands or tens of thousands. The affected PCs cannot be started up. PCs running Windows XP began to fail after they downloaded a virus definitions update file on Friday, May 18. The regular updates are automatically pushed out from Symantec's servers. Users explained that nothing went wrong immediately, but that the next restart showed the infamous Windows 'Blue Screen of Death' instead of the normal start−up sequence. The PCs could not be restored to operation by any normal means. Symantec's China office explained in a statement that the software had mistakenly detected a virus in some key Windows XP system files. These files were either deleted or quarantined.
Source: http://www.vnunet.com/vnunet/news/2190301/millions−pcs−zappe d−bad

**35.** *May 21, VNUNet* — **OpenOffice worm targets Windows, Mac and Linux computers.** A newly discovered worm targeting OpenOffice attempts to download indecent JPEG images onto compromised PCs. Badbunny−A, a macro worm for OpenOffice/StarBasic that drops scripts in other languages, infects computer users when they open an OpenOffice Draw file called badbunny.odg. A macro within the file performs different functions depending on whether the user is running Windows, MacOS or Linux. These can include executing other self−replicating JavaScript and Perl viruses.
Source: http://www.vnunet.com/vnunet/news/2190354/openoffice−worm−do wnloads−bunny

**36.** *May 18, eWeek* — **Hundreds click on 'click here to get infected' ad.** The fact that 409 people clicked on an ad that offers infection for those with virus−free PCs proves that people will click on just about anything. That was evidenced by the 409 people who clicked on an ad that offers infection for those with virus−free PCs. The ad, run by a person who identifies himself as security professional Didier Stevens, reads like this: "Drive−By Download. Is your PC

virus−free? Get it infected here! drive−by−download.info." Stevens, who says he works for Contraste Europe, has been running his Google Adwords campaign for six months now and has received 409 hits. Stevens has done similar research in the past, such as finding out how easy it is to land on a drive−by download site when doing a Google search. Stevens says that he got the idea after picking up a small book on Google Adwords at the library and finding out how easy and cheap it is to set up an ad.
Source: http://www.eweek.com/article2/0,1895,2132447,00.asp

37. *May 18, InformationWeek* — **Online criminal gangs battle with botnets.** Two or three online criminal gangs are waging an all−out battle for control of the largest botnets, sending out waves of malware aimed at stealing zombie computers from rival gangs to build up their own army. Each online gang is trying to build up the biggest botnet because the bigger the army of infected computers they control, the more money spammers and hackers will pay to use them, explains Shane Coursen, a senior technical consultant for Kaspersky Lab. Since the gangs have their own botnets already built up, they're all trying to pilfer victimized computers from their rivals, to diminish their competitor's botnets while they build up their own. Coursen said the author of the well−known Storm Worm, also known as Zhelatin, is going head to head with the author or authors of the Warezov and Bagle worms. It's unclear whether one group is responsible for both the Warezov worm and the Bagle worm or if different groups are behind each one, he said. Regardless, they're both working to steal zombies from the Storm Worm authors.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=XI0ZLCE4XGNGAQSNDLRCKH0CJUNN2JVN?articleID=199601992

**Internet Alert Dashboard**

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

## Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

## General Sector

Nothing to report.
[Return to top]

## DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

### DHS Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

### Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

### Department of Homeland Security Disclaimer